UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

DAVID NOSAL, et al.,

Defendants.
/

No. CR 08-00237 MHP

MEMORANDUM & ORDER

Re: Motion to Dismiss Indictment for Failure to State an Offense

Defendant David Nosal ("Nosal") has been indicted on theft of trade secrets, illegal computer intrusion, and mail fraud. Now before the court is Nosal's second motion to dismiss the Superceding Indictment against him, this time on the alleged basis that none of the twenty counts adequately states an offense. The court has considered the parties' arguments and submissions, and for the reasons stated below, the court issues the following memorandum and order. This order serves to memorialize and supplement the court's ruling on this motion in open court on March 2, 2009.

BACKGROUND[1]

Nosal was a high level executive at an international executive search firm, Korn/Ferry International ("KFI"), from approximately April 1996 to October 2004. KFI was one of the leading providers of executive recruitment services, engaging in searches to fill executive, board-of-director, and similar high level positions, for businesses in the United States. Nosal terminated his employment with KFI in October 2004, with plans to start a competing executive search firm.

Upon his departure, Nosal voluntarily entered into a separation agreement and agreed to serve as an independent contractor to KFI from November 1, 2004 through October 15, 2005. Under the terms of that Separation and General Release Agreement and an Independent Contractor Agreement (collectively, "the Nosal-KFI Agreements"), Nosal agreed to cooperate with KFI on certain ongoing search assignments and agreed not to compete with KFI by not performing executive search, executive placement, management assessment, or management audit services on behalf of any other entity than KFI during the period the Nosal-KFI Agreements were in place. In exchange for his services, Nosal was to receive $25,000 per month during that year, as well as two lump-sum payments on July 31st and October 15, 2005.

Becky Christian was an employee of KFI from approximately September 1999 through January 2005. The individual identified in the Superceding Indictment as "J.F." was employed by KFI from approximately December 1997 to August 2005. J.F. was Nosal's executive assistant prior to Nosal's departure from KFI. According to the Superceding Indictment, both individuals helped Nosal set up his new executive search firm and assisted Nosal in obtaining trade secrets and other things of value from KFI's computer system, prior to and upon termination of their employment with KFI by using their own KFI password-protected user accounts. Specifically, the Superceding Indictment alleges that J.F. and Christian assisted Nosal in obtaining source lists and other custom reports of names and contact information from the KFI "Searcher" database, a highly confidential and proprietary database of executives and companies.

On April 10, 2008, Nosal and co-defendant Becky Christian were charged by indictment with federal statutory violations relating to their alleged involvement in stealing confidential and proprietary information from KFI for the purpose of assisting Nosal in his own executive search activities. On June 16, 2008, the court granted the defendant Christian's motion to sever.

In a June 26, 2008 Superceding Indictment, Nosal was charged with the following offenses:

Count One	18 U.S.C. §§ 1832(a)(5) and 371—Conspiracy to Misappropriate, Receive, Possess, and Transmit Trade Secrets, Gain Unauthorized Access to a Protected Computer, Exceed Authorized Access to a Protected Computer, and Traffic in a Password Allowing Unauthorized Access to a Protected Computer

Counts Two through Nine	18 U.S.C. §§ 1030(a)(4) and (c)(3)(A)—Unauthorized Access to a Protected Computer with Intent to Defraud and Obtaining Something of Value
Count Ten	18 U.S.C. §§ 1832(a)(1), (a)(2), and (a)(4)—Theft, Misappropriation, and Unauthorized Downloading of Trade Secrets
Count Eleven	18 U.S.C. §§ 1832(a)(3) and 1832(a)(4)—Unauthorized Receipt and Possession of Stolen Trade Secrets
Counts Twelve through Nineteen	18 U.S.C. § 1341—Mail Fraud
Count Twenty	18 U.S.C. § 1349—Conspiracy to Commit Mail Fraud

Nosal brings this motion to dismiss the indictment against him, alleging that none of the twenty counts adequately states an offense. Generally, Nosal argues that KFI's allegations involve civil matters and matters of state law and are being improperly raised in the context of a federal criminal prosecution. More specifically, Nosal categorizes the charges into three sets and argues that each set fails to state an offense.

According to Nosal, the first set of charges allege theft and misappropriation of trade secrets in violation of the Economic Espionage Act, 18 U.S.C. section 1832 ("EEA"). Nosal argues that the counts are multiplicitous and neither alleges the required element of the knowledge of illegality of the offense. The government's next set of charges allege that Nosal accessed a computer without authorization in violation of the Computer Fraud and Abuse Act, 18 U.S.C. section 1030 ("CFAA"). Nosal argues that the government only alleges misappropriation and that act is not covered by the CFAA. The government's final set of charges allege that Nosal committed mail fraud by violating the Nosal-KFI Agreements, by failing to disclose that violation, and by continuing to receive monthly payments in the mail. Nosal argues that conduct does not amount to mail fraud because it constitutes an undisclosed breach of contract of an unenforceable contract provision.

The United States opposes Nosal's motion, arguing that Nosal mischaracterizes the charged offenses, all counts are adequately plead, and moreover dismissal of indictments is disfavored as a remedy. The court heard oral argument on the motion on March 2, 2009 and ruled from the bench, denying plaintiff's motion in part and indicating its intent to grant the motion with respect to the mail fraud counts. This memorandum and order provides written detail of that ruling.

LEGAL STANDARD

Under Rule 12(b) of the Federal Rules of Criminal Procedure, a party may file a motion to dismiss based on "any defense, objection, or request that the court can determine without a trial of the general issue." Fed. R. Crim. P. 12(b); United States v. Shortt Accountancy Corp., 785 F.2d 1448, 1452 (9th Cir. 1986). In considering a motion to dismiss, the court is limited to the face of the indictment and must accept the facts alleged in that indictment as true. Winslow v. United States, 216 F.2d 912, 913 (9th Cir. 1955); United States v. Ruiz-Castro, 125 F. Supp. 2d 411, 413 (D. Haw. 2000). A court must decide such a motion before trial "unless it finds good cause to defer a ruling." Fed. R. Crim. P. 12(d); Shortt Accountancy, 785 F.2d at 1452 (citing former Fed. R. Crim. P. 12(e)).

DISCUSSION

I. EEA Charges—Trade Secrets Violations

Taking the three sets of charges in turn, the court begins with the counts alleging trade secrets violations. Nosal argues that counts one, ten and eleven, directed to theft and misappropriation of trade secrets under the EEA, should be dismissed because the government has not alleged the proper mens rea element. The court begins by noting that the EEA on its face requires a "knowing" mens rea element. See 18 U.S.C. § 1832(a).[2] The question before the court is to what aspects of the statute does the knowledge requirement apply, i.e., to what aspects of the statutory text should the word "knowingly" be applied?

Nosal argues the statute must require knowledge of illegal behavior, based on case law suggesting the statute is not necessarily intended to punish competition and that the statutory definition of "trade secret" in the EEA is vague and under-defined. Nosal relies on two cases outside the Ninth Circuit in which defendants unsuccessfully argued the statute was unconstitutionally vague to contend that the EEA must be interpreted narrowly to include an additional mens rea element not specified in the statutory text. See U.S. v. Krumrei, 258 F.3d 535 (6th Cir. 2001) and U.S. v. Hsu, 40 F. Supp. 2d 623 (E.D. Pa. 1999). Nosal concludes the statute, as

interpreted, requires proof of the defendant's knowledge of the illegality of his actions and here, the government failed to allege that Nosal had that knowledge.

The court finds this argument to be without merit. Neither of the two cited cases stand for the stated proposition that the statute requires proof of the knowledge of illegal behavior. In U.S. v. Krumrei, 258 F.3d 535, 536 (6th Cir. 2001), defendant was indicted for violating the EEA, 18 U.S.C. § 1832(a)(2), by knowingly and without authorization transmitting a trade secret to a competitor of the owner. The Sixth Circuit was clear in holding that the statute was constitutional as applied to the defendant because he was well aware of the "proprietariness of the information" he was selling, i.e., that it was a trade secret and he sought to sell it anyway. Id. at 539. Likewise, in Hsu, the court found the statute not unconstitutional as applied to the defendant because the defendant was seeking to acquire that which he knew was not "generally known to" or "readily ascertainable through proper means by, the public." 40 F. Supp. 2d at 631. These holdings make plain it is the knowledge of trade secrets, not the knowledge of illegal behavior, that the EEA requires.

The court notes that all void for vagueness challenges must be unconstitutional as applied to the defendant and "must be examined in light of the facts of the case at hand." Id. at 626-627, citing United States v. Mazurie, 419 U.S. 544, 550 (1975). The question here, therefore, is whether the government's allegations that Nosal knew the source list information and data he took, copied and downloaded from KFI's computer system or otherwise came into possession of via e-mails was proprietary to KFI and that Nosal knowingly stole and possessed information from KFI's computer system anyway, properly states an offense. The court holds that it does.

Further, the court does not find counts ten and eleven multiplicitous. The Superceding Indictment alleges different acts for the two counts, as described above (theft, copying and downloading of KFI source lists in one instance—count ten; and receipt and possession of data from e-mails in another instance—count eleven). While there may be overlapping proof for these counts, the court finds no multiplicity problem because each charge requires proof of an additional fact the other does not. See U.S. v. Garlick, 240 F.3d 789, 794 (9th Cir. 2001) ("The test for multiplicity is whether each count 'requires proof of an additional fact which the other does not.'"). Nosal's objection as to the non-applicability of a duplicative penalty in the statute, because all subdivisions

of section 1832 are published to the same degree, is a matter to be taken up at the time of sentencing. Accordingly, the court DENIES defendant's motion to dismiss counts one, ten and eleven.

II. CFAA Charges—Computer Fraud

Next, Nosal argues that counts two through nine should be dismissed because the Superceding Indictment alleges misappropriation, which Nosal contends is not covered by the CFAA. The provision in question makes it a crime if a person "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . ." 18. U.S.C. § 1030(a)(4). Nosal contends that the terms "without authorization" and "to exceed authorized access" should be read narrowly to exclude the misuse or misappropriation of information obtained with permission.

The Superceding Indictment alleges that two KFI employees, defendant Christian and J.F., used their employee user accounts and passwords to access a protected computer belonging to KFI, and, without authorization and by exceeding authorized access, downloaded, copied and duplicated source lists and other contact information from KFI's proprietary "Searcher" database, and gave that information to Nosal. These actions were allegedly performed for Nosal's benefit and for the purpose of retaining clients and placing candidates as part of non-KFI executive search activities. The government contends these actions were performed conspiratorially, in violation of the Nosal-KFI Agreements and knowingly and with the intent to defraud KFI, in violation of the CFAA. Nosal's position is that the CFAA was aimed primarily at computer hackers and that the statute does not cover employees who misappropriate information or who violate contractual confidentiality agreements by using employer-owned information in a manner inconsistent with those agreements.

Here too, Nosal acknowledges that the law in this area is somewhat unsettled. The Ninth Circuit has not yet ruled on the issue, and courts in other jurisdictions have split views on the question of whether an employee with an improper purpose may be held liable for accessing computer information that s/he is otherwise permitted to access within the scope of his or her employment. Under the CFAA, the term "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the

accesser is not entitled so to obtain or alter." 18 U.S.C.A. § 1030(e)(6). The term "authorization" is not defined by statute. The issue for the court to decide is whether an employee may act "without authorization" or "in excess of authorized access" when he accesses confidential and proprietary business information from his employer's computer that he has permission to access, but then uses that information in a manner inconsistent with the employer's interests or in violation of other contractual obligations, and where the employee intended to use the information in that manner at the time of access.

The parties note the two lines of diverging case law on this issue. Some courts, including two courts of appeal, have broadly construed the CFAA to hold an employee acting to access an employer's computer to obtain business information with intent to defraud, i.e., for their own personal benefit or the benefit of a competitor, act "without authorization" or "exceed authorization" in violation of the statute. See, e.g., Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000); ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006) (Hamilton, J.); Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008); Pac. Aerospace & Elec., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1195-97 (E.D. Wash. 2003); Calyon v. Mizuho Sec. USA, Inc., 2007 WL 2618658, *1 (S.D.N.Y. 2007); Condux Intern., Inc. v. Haugum, 2008 WL 5244818, *4 n3 (D. Minn. 2008) (collecting cases). These courts have generally held that authorized access to a company computer terminated once an employee acted with adverse or nefarious interests and against the duty of loyalty imposed on an employee in an agency relationship with his or her employer or former employer.

Other courts have refused to hold employees with access and nefarious interests within the statute, concluding that a violation for accessing a protected computer "without authorization"or in "excess of authorized access" occurs only when initial access or the access of certain information is not permitted in the first instance. See, e.g., Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 933 (W.D. Tenn. 2008); Diamond Power Intern., Inc. v. Davidson, 540 F. Supp. 2d 1322, 1341-43 (N.D. Ga. 2007); B & B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007);

Brett Senior & Assocs., P.C. v. Fitzgerald, 2007 WL 2043377, *2-4 (E.D. Pa. 2007); Lockheed Martin Corp. v. Speed, No. 2006 WL 2683058, *5 (M.D. Fla. 2006); Int'l Ass'n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005); Bridal Expo, Inc. v. van Florestein, 2009 WL 255862, *10 (S.D. Tex. 2009) (collecting cases). Those courts have generally reasoned that the CFAA is intended to punish computer hackers, electronic trespassers and other "outsiders" but not employees who abuse computer access privileges to misuse information derived from their employment. Nosal argues that reasoning should be followed and the broader "misappropriation" theory of the CFAA should be rejected, because the CFAA was intended to cover "classic" hacking activities over violations of agency or fiduciary duties principles, the plain language targets the unauthorized procurement of information over its wrongful use, and the rule of lenity compels a narrower reading.

The court is not persuaded by Nosal's arguments or by the narrower view of "authorization" embraced in the latter line of cases. As noted by the Third Circuit, "the scope of [the CFAA's] reach has been expanded over the last two decades." P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC., 428 F.3d 504, 510 (3d Cir. 2005). "Employers . . . are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." Id., citing Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003). There is no reason why this expansion should be limited to civil challenges of the unauthorized access of information from a company's computer database by an employee to further a fraud.[3]

Moreover, Nosal errs by focusing exclusively on the later misuse of information by an employee against an employer's interests, in alleged breach of fiduciary duties, while neglecting to address the gravamen of the charge, i.e., the initial access of the employer's computer with the intent to defraud. A CFAA violation under section 1030(a)(4) occurs when a person accesses a protected computer knowingly and with the intent to defraud—which renders the access unauthorized or in excess of authorization—and then, by means of such conduct, the person furthers the intended fraud. The conduct at the heart of the subsection is more than a breach of agent duty. "To be prosecuted

under this section, the use of the computer must be directly linked to the intended fraud. That is, it must be used by an offender ... to obtain property of another, which property furthers the intended fraud." See Manuel of Model Criminal Jury Instructions for the Ninth Circuit, section 8.81 (2004 ed.) ("Computer Fraud—Use of "protected" computer (18 U.S.C. § 1030(a)(4), (e)(2)(A) & (B))"), Comments, citing S. Rep. No. 99–432, at 9 (1986) reprinted in 1986 U.S.C.C.A.N. 2479, 2487.

Likewise, the reasoning underlying the expansion of the CFAA's scope is based on more than agency principles premised on a duty of loyalty; the underpinning of liability here is the required intent to defraud. The Third Circuit divided a claim under CFAA section 1030(a)(4) into four elements: (1) defendant has accessed a "protected computer;" (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so "knowingly" and with "intent to defraud"; and (4) as a result has "further[ed] the intended fraud and obtain[ed] anything of value." P.C. Yonkers, 428 F.3d at 508. Nosal's arguments disregard, or at least marginalize, the third element. The court finds that the intent prong is not to be so lightly read out of a criminal statute, and although much of the case law focuses on civil liability, the CFAA is primarily "a criminal statute, criminalizing and penalizing unauthorized access to computers." Id. at 510; see also Shamrock Foods Co. v. Gast., 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) ("the CFAA is a criminal statute focused on criminal conduct."). Fraud is a meaningful hurdle in criminal law, and the CFAA requires on its face the intent to defraud at the time the protected computer is being accessed. Later misuse of the information alone would not fall within the statute if at the time the employee obtained the information he or she had no intent to use it in a fraudulent way. The government agreed with this statement on oral argument and stated that the CFAA violations are based on the knowing access of electronic records for uses outside their intended purpose.

Here, the government has alleged that the employees' acts of accessing KFI's information were not only purposeful, but also with the intent to defraud, and that confidential and proprietary information was both taken and used to further the intended fraud, i.e., to advance Nosal's own executive search activities, to the detriment of KFI. Christian and J.F. were not authorized to initially access the KFI computer with the intent to defraud KFI. That they accessed the information at issue with nefarious intent rendered the access "without authorization" or "in excess of authorized

access." The First Circuit relied on this definition of "exceeds authorized access" to find the necessary elements for a successful CFAA charge in the employer-employee context in EF Cultural Travel, 274 F.3d at 583-84. In so doing, the First Circuit affirmed that an employee of a tour company acted outside the scope of his confidentiality agreement by providing proprietary information to a competitor tour company employee. Id. The same logic applies with increased force here, not only because Christian and J.F. were bound by confidentiality agreements at the time of the alleged acts, but also because the Nosal-KFI agreements created a continued quasi-employment relationship between Nosal and KFI with additional and ongoing duties of confidentiality and non-competition. See id. at 581 (concluding that appellants' actions had exceeded authorized access "because of the broad confidentiality agreements" that were in place.)

Finally, Nosal's argument concerning the rule of lenity in criminal cases is unavailing because it is only appropriate when there is statutory ambiguity. See U.S. v. Hayes, 129 S.Ct. 1079, 1088-1089 (2009) (the rule applies "only when, after consulting traditional canons of statutory construction, we are left with an ambiguous statute."). The court finds no ambiguity in the statute here. Although no court has heretofore addressed section 1030(a)(4) in the criminal context, ample authority exists to permit criminal actions to proceed based on violations of this section by employees, as interpreted by civil cases, and there is simply no statutory basis to suggest otherwise. See, e.g., Shurgard, 119 F.Supp.2d at 1126 (rejecting contention that section 1030 only applies to "outsiders" and not employees, stating "there is no ambiguity in the statute as to when a party is liable, ("*Whoever* . . . accesses . . .")); see 18 U.S.C. § 1030(a)(4). In sum, because this matter is at the pleading stage and not at the proof stage, the court finds that the government has sufficiently set forth its allegations of the misuse of confidential information having been obtained through access to the KFI's computer system that charges CFAA violations. Accordingly, the court DENIES defendant's motion to dismiss counts two through nine.

III. Mail Fraud Charges

Nosal argues the mail fraud conspiracy and substantive charges in counts twelve through twenty should be dismissed because they improperly seek to cover a civil matter—breach of contract. Nosal contends the government's mail fraud charges are based solely on Nosal having

allegedly committed fraud by deceiving KFI about the fact that he was conducting his own executive-search-related activities during the period the Nosal-KFI Agreements were in place. Nosal argues that any alleged breach of his agreement not to compete with KFI by not performing executive search and other services on behalf of any other entity during the period the Nosal-KFI Agreements were in place is a breach of contract claim and not a federal crime. Nosal further argues the mail fraud charges should be dismissed because they rest on alleged fraud arising out of a contractual non-compete provision that is invalid under California law.

Nosal is charged with mail fraud and conspiracy to commit mail fraud under 18 U.S.C. sections 1341 and 1349, respectively. To prove a violation of the mail fraud statute, the government must show that (1) the defendant formed a scheme to defraud; (2) the defendant used the United States mails or caused a use of the United States mails in furtherance of the scheme; and (3) the defendants did so with the specific intent to deceive or defraud. See Schreiber Distribut. Co. v. Serv-Well Furniture Co., Inc., 806 F.2d 1393, 1399-1400 (9th Cir. 1986). The mail fraud statute has been broadly construed by the courts, given that the purpose of the statute is to proscribe the use of the mails "in any situation where it is closely entwined with fraudulent activity." Id., citing United States v. Halbert, 640 F.2d 1000, 1009 (9th Cir. 1981).

Here, the Superceding Indictment alleges that Nosal committed mail fraud by engaging in a scheme to defraud KFI by means of false and fraudulent misrepresentations and promises. Specifically, Nosal is alleged to have provided materially false information to, and purposefully omitting and concealing material information from, KFI regarding Nosal's executive-search-related activities that were in violation of the Nosal-KFI Agreements. It was allegedly part of the scheme that Nosal and Christian directed others to take without authorization and in excess of authorized access confidential and proprietary information and trade secrets from KFI's computer system with the intent to defraud, and subsequently used that information to conduct executive searches and related activities. Also part of the alleged scheme was that Nosal misrepresented on numerous occasions to KFI executives that he was complying with the Nosal-KFI Agreements, so that he could both continue to receive his monthly independent contractor payments and remain eligible to receive

his lump-sum payments under the agreements. The alleged use of the mails in furtherance of the scheme to defraud consists of eight monthly payment checks that were mailed by KFI to Nosal.

The government contends that because Nosal caused the checks to be mailed for the purpose of executing his scheme to defraud, this is sufficient to support the charges under examination here. On oral argument, the government asserted that evidence of the conspiracy to commit mail fraud charge is provided by the bi-weekly telephone calls between Nosal and KFI executive in which Nosal falsely told KFI he was complying with the Nosal-KFI agreements. The court disagrees that these allegations of Nosal having mislead KFI support the charges.

The government relies at least in part on the theory of deprivation of honest services, describing in its brief and on oral argument Nosal's alleged scheme to deprive KFI of his honest services as an independent contractor for the purpose of the charges at hand. However, the Superceding Indictment fails to make any such allegations, relying on the false and fraudulent pretenses theory instead. Furthermore, the honest services doctrine has mainly been used to punish fraud against citizens perpetrated by government officials. See, e.g., U.S. v. Kincaid-Chauncey, 556 F.3d 923, 939 (9th Cir. 2009), citing U.S. v. Silvano, 812 F.2d 754, 759 (1st Cir. 1987) ("the theory relies on the idea that 'a public official acts as 'trustee for the citizens and the State . . . and thus owes the normal fiduciary duties of a trustee, e.g., honesty and loyalty to them.'") While honest services fraud can occur in the employer-employee relationship, courts have been hesitant to impose federal liability upon every private dispute involving an employee transgression that incurs no public deprivation of rights. See, e.g., U.S. v. Czubinski, 106 F.3d 1069, 1077 (1st Cir. 1997) (holding that examining confidential information for one's own purposes dues not rise to the requisite level of a workplace violation to sustain a mail fraud charge under the honest services theory).

The government acknowledges that the mail fraud statute may not reach every private business practice that involves a deprivation of honest services through a breach of contract or of a fiduciary duty. On the state of the Superceding Indictment before this court, that acknowledgment is of no moment since the government has not alleged an honest services theory. What the government does argue is that the mail fraud statute reaches breaches of contract or of a fiduciary duty where there was a recognizable scheme to defraud and where the defendant made fraudulent

representations reasonably calculated to deceive. This is nothing more than a false and fraudulent pretense theory and on this theory the allegations of the Superceding Indictment fall short. The fraudulent representations that are calculated to deceive must also be performed in specific furtherance of the scheme. Nosal's acquiescence in allowing KFI to mail the monthly payment checks to his home does not contain sufficient deception to bring it within the purview of the mail fraud statute. The Nosal-KFI Agreements were broad and while certain of Nosal's alleged actions may have been misleading, there is a dearth of allegations regarding intentional and specific misrepresentations of fact made to further the fraudulent scheme. Accordingly, the mail fraud charges cannot be sustained.

The court need not reach Nosal's argument regarding the validity of non-competition clauses under California law and whether an undisclosed breach of such a provision can constitute fraud. The court finds that the government has failed to allege a scheme to defraud that involves the use of the mails in furtherance of the scheme and the specific intent to defraud. Even accepting the allegations of the indictment as true, the government has insufficiently pled the elements of mail fraud to withstand a motion to dismiss. The mail fraud charges must be dismissed because the law is clear that the prosecution cannot cure defects in an indictment by providing more particularized notice subsequent to the indictment. See Russell v. U.S., 369 U.S. 749, 770 (1962) ("a bill of particulars cannot save an invalid indictment . . . [f]or a defendant could then be convicted on the basis of facts not found by, and perhaps not even presented to, the grand jury which indicted him.") Accordingly, the court GRANTS defendant's motion to dismiss counts twelve through twenty of the Superceding Indictment.

CONCLUSION

For the reasons set forth above, the court **DENIES in part** and **GRANTS in part** defendant's motion to dismiss the indictment for failure to state an offense. The court DENIES defendant's motion to dismiss counts one through eleven and GRANTS defendant's motion to dismiss counts twelve through twenty of the Superceding Indictment.

IT IS SO ORDERED.

Dated: April 13, 2009

MARILYN HALL PATEL
United States District Court Judge
Northern District of California

ENDNOTES

1. The facts relevant to the instant motion were reviewed during the March 2, 2009 hearing, therefore, only a summary is necessary here. Unless otherwise noted, all cited facts are taken from the Superceding Indictment (Docket No. 42) and are not disputed for purposes of the instant motion.

2. Section 1832(a) of the EEA provides:

> (a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a). Nosal is charged with violations of all five subsections.

3. The CFAA lists seven different types of conduct punishable by fines or imprisonment, which are set forth in 18 U.S.C. section 1030(c). Counts two through nine of the Superceding Indictment charge Nosal under subsection 1030(c)(3).